Tech Talks: Own Your Data (Apple/Android)

Know the apps and settings for increasing your privacy

Privacy Apps (Search, Share, Store)

Basic/Intermediate

- **Private Browser** (e.g. Brave): Blocks trackers and doesn't save your history
- **Private Search Engine** (e.g. DuckDuckGo): Avoid ad tracking and personal profiling with an anonymous search engine
- **Private Messaging/Calling** (e.g. Signal): Have private conversations using encrypted direct messaging app
- **Standard File Storage/Sharing** (e.g. iCloud or Google Drive): Files encrypted in transit and rest - Storage companies reserve the right to access/scan files for illegal content

More Advanced

- **Secure File storage** (e.g. Tresorit): Specialized services can be used for encrypting file sharing and storage
- **Encrypted Email** (e.g. Protonmail): Improve private and secure communications with encrypted email service
- **Virtual Private Network** (e.g CyberGhost): Encrypt your data and mask your location for anonymous browsing
- **TOR Browser** (e.g. OrNET): Hide your IP address through layers of encryption and random relays through a large network of servers

Apple Settings

Settings > Privacy

- Location Services
- Microphone
- Camera
- Photos

  (and more areas)

Settings > Safari > Search Engine > DuckDuckGo

Settings > Safari > Settings for websites

- Camera, Microphone, Location
- Privacy & Security Settings
- Advanced > Website Data

Android Settings

Settings > Privacy > Permission manager

- Location
- Microphone
- Camera

  (and more areas)

Chrome App > Three dot menu > Settings > Search Engine > DuckDuckGo

Google (app) > Manage your Google Account (top right) > Data & Personalization

- Web and App Activity
- Location History
- YouTube History
- Ad Personalization

SANTA CRUZ PUBLIC LIBRARIES

updated 10/27/2021

Tech Talks: Own Your Data (Apple/Android)

Know the apps and settings for increasing your privacy

More Terms

- **IP (Internet Protocol) Address** - Identifying number assigned to each device
- **ISP (Internet Service Provider)** - Business used for accessing and using the Internet
- **DNS Servers** - Phone book of the Internet, translates human readable domain names to computer readable IP addresses
- **Internet Browser** - Software application used to access information on the Internet
- **Cookies** - Data packets exchanged between servers and browsers to identify users and track activity
- **Metadata** - data about data
- **Data Mining** - Finding patterns and connections in data to create new information
- **Behavioral Advertising** - Ads served based on data collected over time
- **Contextual Advertising** - Ads served based on keywords used
- **Advertising Identification** - Unique identifier used to build personal ad profile
- **End-to-End Encryption (E2EE)** - Data encrypted in a way that allows only the unique recipient of a message to decrypt it
- **TOR (The Onion Router)** - Data encapsulated in layers of encryption and routed randomly through a network of servers to ensure anonymity
- **VPN** - Service that encrypts your data and masks your location for anonymous browsing
- **California Consumer Privacy Act (CCPA)** - Provide CA residents with following abilities:
    - Know what personal data is being collected about them
    - Know whether their personal data is sold or disclosed and to whom
    - Say no to the sale of personal data
    - Access their personal data
    - Request a business to delete any personal information about a consumer collected from that consumer
    - Not be discriminated against for exercising their privacy rights

Resources

- Privacy Planner - https://securityplanner.consumerreports.org
- Virtual Privacy Lab - https://www.sjpl.org/privacy

SANTA CRUZ PUBLIC LIBRARIES

updated 10/27/2021